**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT) -

| (51) International Patent Classification 6 : | | (11) International Publication Number: | WO 99/39505 |
|---|---|---|---|
| H04N 7/18, 9/47, 7/10, 7/14 | A1 | (43) International Publication Date: | 5 August 1999 (05.08.99) |

(21) International Application Number: PCT/US99/01803

(22) International Filing Date: 27 January 1999 (27.01.99)

(30) Priority Data:
09/015,674 29 January 1998 (29.01.98) US

(71)(72) Applicant and Inventor: KAVY, Sol, Frank [US/US]; 901 Menlo Oaks Drive, Menlo Park, CA 94025 (US).

(74) Agents: SALTER, James, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

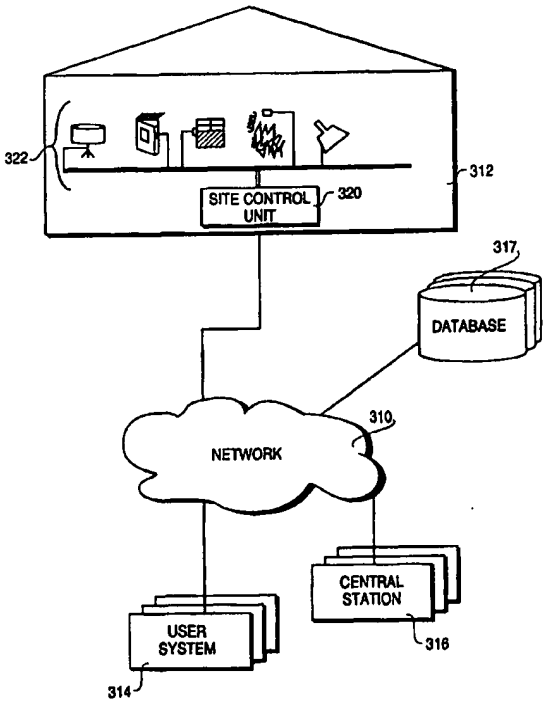
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: NETWORKED SECURITY SYSTEM FOR NETWORK-BASED MONITORING AND CONTROL OF AN ENVIRONMENT

(57) Abstract

A networked security system for network-based monitoring and control of an environment is disclosed. The networked security system includes: 1) a site control unit (320) for monitoring and controlling devices (322) in an environment, the site control unit (320) further includes a site system controller for assembling device information into data packets for transfer on a network (310); and, 2) a user system (314) connected with the site control unit (320) via the network (310) for receiving the data packets from the site control unit (320) via the network (310) and for processing the data packets for access for networked user.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

# NETWORKED SECURITY SYSTEM FOR NETWORK-BASED MONITORING AND CONTROL OF AN ENVIRONMENT

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

The present invention relates to the field of security systems, computer networks, and remote control systems.

### 2. Description of Related Art

Conventional security monitoring and control systems typically use direct point-to-point connections between a monitored location and a central control facility. In many of these conventional systems, a hard-wired direct connection between a site control unit at the monitored location and the central control facility is used. In other conventional systems, a point-to-point telephone line is used to transmit data between a control device at the monitored location and the central monitoring facility via a modem. In still other conventional applications wireless transmission and receiving apparatus is used to transmit security data between a monitored location and a central control facility. In many circumstances, however, the bandwith limitations imposed by the wireless apparatus or the telephone infrastructure limits the amount and type of data that can be transmitted from the monitored location and the control facility. For example, many of these prior art systems are unable to transmit video as part of the transmitted security information.

Although these conventional security systems provide a means for transmitting security information to a remote location, the remote location cannot be arbitrarily defined. For example, many security systems are configured to dial out to a particular telephone number at a predefined location. These systems do not provide a convenient way for relocating a control facility to a different site or to any arbitrary site. Similarly, the hard-wired systems require expensive

reconfiguration if either the control facility or the monitored location is moved. Moreover, the prior art security systems suffer bandwidth limitations and the need for expensive transmission apparatus.

There are several types of networked security systems in the prior art. U.S. Patent No. 4,876,597, assigned to ADT Security Systems, Inc., Parsippany, New Jersey ('597 herein), is representative of one type of prior art system. The '597 patent describes a video observation system wherein a scene to be monitored at a remote location is captured as a series of still images. The monitoring of freight trains is cited as an application of this system. If the observer is at a location remote from the point at which the images are taken, the patent states that various techniques can be used to facilitate transmission of the image information (preferably in digital form) through relatively low cost transmission links such as voice grade telephone lines. This patent represents conventional systems that use telephone lines for the transmission of security data from a monitored location to a control facility.

U.S. Patent No. 5,699,276 describes a utility meter interface apparatus for measuring utility usage at a residential location. A computer is connected to the utility meter and provides an interface between a communication network and a device located inside the home. The disclosed system relates to remote utility meter reading and remote load management. The system includes a network interface that may be coupled to a digital service network, that communicates, for example, via satellite, wireless communication, fiber-optic cables, coaxial cables, or twisted pair telephone lines. Although this system describes the use of various types of network infrastructures, the system nevertheless is confined to a predefined relation between the monitored location and the control facility.

U.S. Patent No. 5,684,799 describes a full-service network having a distributed architecture. The video distribution network consolidates video streams from different information providers and outputs a consolidated signal onto a transport ring. The digital information is transmitted using asynchronous

transfer mode (ATM) and RF distribution over a hybrid-fiber-coax local loop distribution. Again, this patent describes a system using an expensive proprietary network infrastructure.

U.S. Patent No. 5,675,390 describes a home entertainment system combining complex processor capability with a high-quality display. This patent relates to a home entertaining system having a high-quality monitor to display digitally received broadband video without a loss of signal quality. The system provides a multipurpose computer system to control consumer electronics such as a large monitor or television. The circuitry also provides audio and video tuning capability. In one described embodiment, high-quality video signals are received from satellites broadcasting digital video signals, digital cable signals, and other wireless digital broadcasts. A computer system with a card inserted therein includes a satellite tuner, digital demodulator, and a means to capture video, audio, and data in a form which a personal computer can process. The system also provides support for remote control of both the personal computer and the monitor functions in the personal computer.

U.S. Patent No. 5,648,966 describes a method of sending an alarm to a network management station when an unusual event occurs in a managed network station. This patent represents a class of technology related to the administration of a computer network. These specialized network management systems provide a means for detecting network errors and for performing predefined procedures or notifications as a result of a network error. These systems are not analogous to the residential or commercial security monitoring and control of the present invention.

Thus, a networked security system for network-based monitoring and control of an environment is needed.

## SUMMARY OF THE INVENTION

A networked security system for network-based monitoring and control of an environment is disclosed. The networked security system includes: 1) a site control unit for monitoring and controlling devices in an environment, the site control unit further includes a site system controller for assembling device information into data packets for transfer on a network; and, 2) a user system connected with the site control unit via the network for receiving the data packets from the site control unit via the network and for processing the data packets for access by a networked user.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a prior art computer network topology.

Figure 2 illustrates the prior art architecture of a conventional computer system.

Figure 3 illustrates the computer network architecture of the preferred embodiment.

Figure 4 illustrates the network structure of the present invention in more detail.

Figure 5 illustrates the site system controller software architecture.

Figure 6 illustrates the central station software architecture.

Figures 7-11 are flowcharts illustrating the processing logic used by the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a networked security system for network-based monitoring and control of an environment. In the following detailed description,

numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that these specific details need not be used to practice the present invention. In other circumstances, well known structures, materials, circuits, and interfaces have not been shown or described in detail in order not to unnecessarily obscure the present invention.

Referring now to Figure 1, a diagram illustrates the network environment in which the present invention operates. In this conventional network architecture, a server computer system 100 is coupled to a wide-area network 110. Wide-area network 110 includes the Internet, or other proprietary networks including America On-Line™, CompuServe™, Microsoft Network ™, and Prodigy ™, each of which are well known to those of ordinary skill in the art. Wide-area network 110 may include conventional network backbones, long-haul telephone lines, Internet service providers, various levels of network routers, and other conventional means for routing data between computers. Using conventional network protocols, server 100 may communicate through wide-area network 110 to a plurality of client computer systems 120, 130, 140 connected through wide-area network 110 in various ways. For example, client 140 is connected directly to wide-area network 110 through direct or dial up telephone or other network transmission line. Alternatively, clients 130 may be connected through wide-area network 110 using a modem pool 114. A conventional modem pool 114 allows a plurality of client systems to connect with a smaller set of modems in modem pool 114 for connection through wide-area network 110. In another alternative network typology, wide-area network 110 is connected to a gateway computer 112. Gateway computer 112 is used to route data to clients 120 through a local area network 116. In this manner, clients 120 can communicate with each other through local area network 116 or with server 100 through gateway 112 and wide-area network 110.

Using one of a variety of network connection means, server computer 100 can communicate with client computers 150 using conventional means. In a particular implementation of this network configuration, a server computer 100 may operate as a web server if the World-Wide Web (WWW) portion of the Internet is used for wide area network 110. Using the HTTP protocol and the HTML coding language across wide-area network 110, web server 100 may communicate across the World-Wide Web with clients 150. In this configuration, clients 150 use a client application program known as a web browser such as the Netscape™ Navigator™ published by Netscape Corporation of Mountain View, CA, the Internet Explorer™ published by Microsoft Corporation of Redmond, Washington, the user interface of America On-Line™, or the web browser or HTML translator or any other well-known supplier. Using such conventional browsers and the World-Wide Web, clients 150 may access graphical and textual data provided by web server 100. Conventional means exist by which clients 150 may supply information to web server 100 through the World- Wide Web 110 and the web server 100 may return processed data to clients 150.

Having briefly described one embodiment of the network environment in which the present invention operates, Figure 2 illustrates an example of a computer system 200 illustrating an exemplary client 150 or server 100 computer system in which the features of the present invention may be implemented. Computer system 200 is comprised of a bus or other communications means 201 for communicating information, and a processing means such as processor 202 coupled with bus 201 for processing information. Computer system 200 further comprises a random access memory (RAM) or other dynamic storage device 204 (commonly referred to as main memory), coupled to bus 201 for storing information and instructions to be executed by processor 202. Main memory 204 also may be used for storing temporary variables or other intermediate information during execution of instructions by processor 202. Computer system 200 also comprises a read only memory (ROM) and /or other static storage device

206 coupled to bus 201 for storing static information and instructions for processor 202.

An optional data storage device 207 such as a magnetic disk or optical disk and its corresponding drive may also be coupled to computer system 200 for storing information and instructions. Computer system 200 can also be coupled via bus 201 to a display device 221, such as a cathode ray tube (CRT) or a liquid crystal display (LCD), for displaying information to a computer user. For example, graphical depictions of a business card and other types of graphical or textual information may be presented to the user on display device 221. Typically, an alphanumeric input device 222, including alphanumeric and other keys is coupled to bus 201 for communicating information and/or command selections to processor 202. Another type of user input device is cursor control device 223, such as a conventional mouse, trackball, or other type of cursor direction keys for communicating direction information and command selection to processor 202 and for controlling cursor movement on display 221.

Alternatively, the client 150 can be implemented as a network computer or thin client device, such as the WebTV Networks™ Internet terminal or the Oracle™ NC. Client 150 may also be a laptop or palm-top computing device, such as the Palm Pilot™. Such a network computer or thin client device does not necessarily include all of the devices and features of the above-described exemplary computer system; however, the functionality of the present invention may nevertheless be implemented with such devices.

A communication device 225 is also coupled to bus 201 for accessing remote computers or servers, such as web server 100, or other servers via the Internet, for example. The communication device 225 may include a modem, a network interface card, or other well known interface devices, such as those used for interfacing with Ethernet, Token-ring, or other types of networks. In any event, in this manner, the computer system 200 may be coupled to a number of

servers 100 via a conventional network infrastructure such as the infrastructure illustrated in Figure 1 and described above.

The present invention includes hardware and various processing steps, which will be described below. The steps of the present invention may be embodied in machine or computer executable instructions. The instructions can be used to cause a general purpose or special purpose processor, which is programmed with the instructions to perform the steps of the present invention. Alternatively, the steps of the present invention may be performed by specific hardware components that contain hard wired logic for performing the steps, or by any combination of programmed computer components and custom hardware components. While embodiments of the present invention will be described with reference to the World-Wide Web, the method and apparatus described herein is equally applicable to other network infrastructures or other data communications systems.

Referring now to Figure 3, a preferred embodiment of the network configuration of the present invention is illustrated. In the preferred embodiment, users at one of a plurality of user systems 314 and administrators at one of a plurality of central stations 316 may access one of a plurality of site control units 320 to monitor and control devices 322 at one of a plurality of sites 312 being monitored via the Internet 310. User system 314 can be used by anyone authorized to access devices 322 at site 312. There can be one or a plurality of user systems 314. The term "users" or "system users" denotes herein an operator of a user system 314. Central station 316 is an administration site, which validates the operation of the networked security system and the authority of those using the system. There can be one or a plurality of central stations 316. The term "administrator" or "central station user" denotes herein an operator of a central station 316. The central station 316 uses one or a plurality of databases 317 either resident within central station 316 or, as shown in Figure 3, residing on a network-accessible database server 317. The database 317 is used for storage of

device status information from monitored site 312 or user information related to users of user system 314. Database 317 may be any of a variety of conventional ODBC-compliant databases, such as Microsoft Access, Oracle 8, or a SQL server. It will be apparent to those of ordinary skill in the art that database 317 may represent a plurality of databases. Providing a plurality of databases allows the system to support a plurality of redundant central stations 316.

As described above, user system 314 and central station 316 may be implemented as conventional computer systems with network access capability, such as the exemplary system shown in Figure 2. Site control unit 320 may also be implemented as a conventional computer system, a conventional alarm panel, or a set-top box as described above. Software for implementing the present invention runs on user system 314, central station 316, and on site control unit 320.

In general, the present invention provides a means and method for networked-based monitoring and control of a site accessible via the Internet. The preferred embodiment can be connected to the Internet and a conventional alarm panel. The system performs the control functions and makes monitoring information available to any authorized users on the Internet. For commercial users, the system is typically connected to a local LAN 116 and data packets are routed onto the Internet. For residential users, the system may connect directly to the Internet via a conventional Internet service provider (ISP), or users may connect to the Internet through central station 316, which may act as an ISP using conventional methods. In either case, a networked security system for network-based monitoring and control of an environment is provided. The networked security system includes: 1) a site control unit for monitoring and controlling devices in an environment, the site control unit further includes a site system controller for assembling device information into data packets for transfer on the network; and, 2) a user system connected with the site control unit via the

network for receiving the data packets from the site control unit via the network and for processing the data packets for access by a networked user.

It is important to distinguish two basic models for accessing the monitored site 312 through the Internet. First, in a self-monitoring model, users of user systems 314 communicate through the Internet directly with a Web server within site control unit 320. In this manner, a user may directly monitor or control devices at a site 312 of interest. Using the system components described below, the user in a self-monitoring model is presented with a user interface on user system 314 providing the user with a full set of controls and real-time monitoring and status information for monitoring and controlling site 312.

The second type of access model is a station monitoring model. In the station monitoring model, a Web server within central station 316 collects information from site control unit 320 and stores this information in a database 317. This collected information includes configuration and status information for the site control unit and user information including account and user configuration information. The database 317 allows central station 316 to maintain complete and current status, as well as a status history, for all monitoring and control devices 322 at monitored site 312. Given that there may be many monitored sites 312, central station 316 keeps the information in database 317 up to date for each of the plurality of monitored sites 312. Users of user systems 314 may directly access the site control unit 320 in self-monitoring model, or users may query the status of a monitored site 312 by querying database 317 updated as a result of the station monitoring model.

Referring now to Figure 4, an architectural block diagram illustrates in detail the functional blocks of the preferred embodiment. On the user side, the user system 314 computing system includes a Web interface 414, which includes a conventional Web client. The Web Interface 414 may be implemented on a standard browser 416, such as one of the browsers listed above. These components provide network 310 or Internet access for the user system 314. By

use of these components, a user is presented with and able to manipulate a graphical user interface (GUI) generated by the site control unit 320 in a manner described in more detail below. The user of user system 314 may also access database 317 via network 310.

As illustrated in Figure 4, the site control unit 320 at the site 312 being monitored or controlled includes a site system controller 420. The site system controller 420 contains the bulk of the software for driving the system of the present invention. This software is described in more detail below in connection with Figure 5.

The site system controller 420 can be coupled with several different types of conventional devices for controlling a variety of different types of monitoring and control devices. For example, as shown in Figure 4, site system controller 420 can be coupled with a conventional alarm panel 430, which is coupled with an array of conventional monitoring and control devices 322. In the preferred embodiment, several conventional alarm panels 430 may be used, such as the FE100 or 685 units by Ademco™, the Martonics, SAFECOM, or Concept 1000/2000/3000 panels. In general, these conventional alarm panels include at least two external interfaces: a control interface 428 and a telephone line interface 427. As well known to those of ordinary skill in the art, the control interface 428 is a standard interface using a conventional protocol for enabling the alarm panel 430 to be programmed and controlled by a field service engineer. This control interface 428 is connected with a compatible interface in the site system controller 420. The telephone line interface 427 of the alarm panel is also a conventional alarm panel interface for reporting digital alarm and status information to a central facility. In the preferred embodiment, this telephone interface is connected to a compatible interface of the site system controller 420. In the preferred embodiment, several conventional monitoring and control devices 322 may be used with the present invention. These control devices 322 include, but are not limited to: window / door sensors, door openers, access

control devices, fire / smoke / chemical / temperature / pressure detectors, electro-mechanical devices, lights, automatic sprinklers, and keypads. In addition, the monitoring and control devices 322 include other types of devices including video cameras or other video sources, video cassette recorders (VCRs), audio sources, infrared (IR) programmable devices, or other types of monitoring or control devices. It will be apparent to those of ordinary skill in the art that the functionality of the site system controller 420 and the functionality of the alarm panel 430 may be integrated into a single unit.

As shown in Figure 4, site system controller 420 can also be coupled with a conventional device controller 432, such as a CM11A device controller manufactured by X-10 (USA) Inc. of Closter, NJ. Such conventional devices may be programmed to control a variety of devices 322, such as the devices set forth be example above. These control devices 432 typically include a serial data interface for transferring data and control messages to/from the device. In the preferred embodiment, the site system controller 420 is coupled to the conventional device controller 432 via this serial interface. It will be apparent to those of ordinary skill in the art that a variety of conventional control devices may be coupled to the site system controller 420 using conventional types of interfaces.

The site system controller 420 may also be configured to include a conventional video controller card 434, a conventional audio controller card 436, and a conventional IR controller card 438. These controllers, typically implemented as circuit cards housed within site system controller 420, may be used to receive and process corresponding video and audio data from devices 322. The conventional IR controller 438 may be used to produce IR command signals for programming devices 322 having an IR receiver. Controllers 434, 436, and 438 typically include firmware or software drivers for programming the controllers via software within site system controller 420. It will be apparent to one of ordinary skill in the art that one or more of the control devices 430, 432,

434, 436, or 438 may not be present in a particular implementation, yet the present invention still retains a level of functionality corresponding to the included control devices.

Site System Controller Software

Referring now to Figure 5, the site system controller 420 software architecture 520 is illustrated. The site system controller software 520 includes an embedded Web server 424 for accepting service requests from a user system 314 or a central station 316. This software component may be implemented using a conventional Personal Web Server as developed by Microsoft Corporation of Redmond, Washington or the WebSite Server produced by O'Reilly Associates. The site system controller software 520 also includes an embedded event server 512. The event server 512 provides a means by which the site system controller 420 automatically obtains updated status information from one or more control devices 322 and forwards the status information to one or more central stations 316 or one or more databases 317 at pre-configured time intervals.

The site system controller software 520 further includes a graphical user interface generator (GUI) 513 for providing a user with a graphical means for monitoring and controlling the environment at the site 312. The graphical user interface generator 513 of the site system controller software 520 includes a means for displaying and controlling the selection and manipulation of abstraction images or icons that represent objects familiar in the site 312 setting. These abstractions can be manipulated by the user to activate and control corresponding control devices 322 at the site 312. The abstraction images and the other displayed components of the GUI 513 are constructed mainly in the site system controller 420 as conventional Web pages coded in a conventional coding language such as the Hypertext Markup Language (HTML). These Web pages of GUI 513 are transferred to user system 314 or central station 316 via network 310 and displayed to a user or administrator via the browser 416.

The site system controller software 520 further includes a Common Application Language Interface 514 (CAL) published by the CEBus Committee of the Electronic Industry Association (EIA), Specification EIA-600, first published in 1992. This conventional interface provides a generic object interface for manipulating objects corresponding to control devices 322, or portions thereof. The CAL interface is also described in the "CEBus Standard User's Guide, Grayson Evans, May, 1996. The CAL interface is a basic description of a set of abstract base classes for Object Oriented programming. The base classes detail the data and methods for representing monitoring/control devices such as, televisions, VCRs, lights, dimmers, and security panels. If necessary, the CAL interface 514 translates a user or administrator action request into one or more device controller-specific commands for implementing the action request on a particular set of installed device controllers 321. In the preferred embodiment, Common Object Modules (COM or DCOM) are used to invoke the appropriate CAL object interface corresponding to the particular action request. COM is a conventional methodology (or approach to programming) in which the implementation and the interfaces are separated in a very specific manner. The approach yields a true separation between how something works and the interface to it. COM is often used for programming in a Microsoft Win32 Application Program Interface (API). It allows different versions of systems to co-exist on the same platform. A description of the conventional COM system is found in, "Dale Rogerson; Inside COM, Microsoft's Component Object Model; Microsoft Press; 1997."

The site system controller software 520 further includes a real time event manager 516 for responding to alarms and other events occurring in one or more of the control devices 322. The real time event manager 516 receives an alert from one or more control devices 322 via a device controller 321 and performs one or more tasks or actions in response to the alert. The tasks performed in response to a particular alert are pre-configured in the real time event manager

516 by the administrator. The tasks may include: sending an email message to a defined address, calling a pager, sending an error message, posting a database entry, or other types of actions.

The site system controller software 520 further includes a device model 518 for handling the device controller specific interfaces. For example, a particular device controller 321 may be an X10 device having an X10 type interface. Alternatively, a LonWorks controller having a LonWorks interface developed by Echelon Corporation, Palo Alto, Ca. may be used. The device model 518 insulates the higher level software components of the site system controller software 520 from the device-specific details of the device controller 321 interface.

The site system controller software 520 is supported in the preferred embodiment by the Windows 95 or Windows CE operating system 505 developed by Microsoft Corporation of Redmond, Washington. The Windows operating system is well-known to those of ordinary skill in the art. The operating system 505 of the preferred embodiment includes a conventional Secure Socket Layer (SSL) 506 component for handling secure data transfers between the site control unit 320 and user system 314 or central station 316.

Referring now to Figure 6, the software components 610 of the central station 316 are illustrated. In the preferred embodiment, the central station 316 may act as a Web client or a Web server. For this reason, the central station contains both a conventional Web client 614 and a Web server 612. Both the Web server 612 and the Web client 614 are layered on a conventional browser 616 as described above. The central station 316 also includes a database server 618 for accessing database 317. As described above, database 317 is used for storage of device status information and user information. The Web server 612 of the central station 316 is used to collect information from the site control unit 320 and to cause the storage of this collected information into the database 317. The Web client 614 of the central station 316 is used to access the database 317 to retrieve

and display device or user information. The Web client 614 is further used to directly access a site control unit 320 to configure a device, check status of a device, or control a device at a monitored site 312. It will be apparent to those of ordinary skill in the art that the software components of the central station 316 and database 317 may be implemented on the same hardware platform or different hardware platforms as desired in a particular implementation.

Referring now to Figures 7-11, flowcharts illustrate the processing logic of the present invention. Figures 7-9 illustrate the interaction between the processing logic in the user system 314 and the site system controller software 520 for implementing the preferred embodiment. Figures 10 and 11 illustrate the interaction between the processing logic in the central station 316 and the site system controller software 520 for implementing the preferred embodiment.

Referring now to Figure 7, the first portion of the processing interaction between the user system 314 and the site system controller software 520 is illustrated. Initially, a user at user system 314 invokes a conventional browser 416 (block 710). The browser makes a request to a Domain Name Server (DNS) for a look-up of the requesting user's name. In addition, an IP address of a site control unit corresponding to the user is obtained from the DNS (block 715). The user system 314 then makes an access to the user's site control unit 320 (SCU) using the retrieved IP address. In response, the Web server 424 of the SCU 320 returns a challenged-based request to the user system 314 via a Secure Socket Layer (SSL) 506 transaction (block 720). SSL is a conventional protocol. In response to the challenged-based request from the SCU 320, the user system 314 responds to the SCU 320 with a secure response that requests access to the SCU 320 by the user of user system 314 (block 725). If the user is granted access to the SCU 320 on the basis of previously established authorization criteria for the user, processing path 735 is taken to the bubble labeled A shown in Figure 8. If access to the SCU 320 is denied, processing path 740 is taken back to block 715 where the user may enter new identifying information to obtain access to the SCU 320.

Referring now to Figure 8, processing for the user system / site control unit processing continues at bubble A. At this point, the user has gained access to his/her SCU 320 via the browser of user system 314. The GUI 513 of site control unit 320 responds to the user system 314 access with the first of a set of HTML encoded Web pages of the SCU graphical user interface (GUI 513). These Web pages are transferred to the user system 314 and displayed by browser 416 (block 810). Using conventional browser tools, the user may navigate through these Web pages of GUI 513 and select one or more of the symbols and objects presented on these Web pages (block 815). The symbols and objects generated by GUI 513 and displayed at the user system 314 represent abstraction symbols and objects that each correspond to an individual or set of control devices supported by that particular site control unit 320. The user may navigate to a particular abstraction symbol of interest and select the abstraction symbol using browser 416 (block 820). In response to the selection of the abstraction symbol at user system 314, an action request message is sent to the site control unit 320 (block 820). In response to the receipt of an action request message, the SCU 320 invokes a CAL object interface corresponding to the action request message, which corresponds to the selected abstraction symbol (block 825). The invoked CAL object interface of CAL Interface 514 causes a message to be sent to activate a corresponding driver interface through device model 518 (block 830). The activated driver interface corresponds to the action request received from the user system 314. The activated driver interface activates a corresponding driver and causes the driver to issue a controller level command to perform the specified action on the specified control device of control devices 322 through controllers 321. The specified action and the specified control device is identified using information in the action request message. Subsequently, hardware performs the controller level command to complete the specified action on the specified control device (block 835). Processing continues at the bubble labeled B shown in Figure 9.

Referring now to Figure 9, processing for the user system / site control unit processing continues at bubble B. At this point, the user has selected an abstraction symbol on the user system 314 and caused a corresponding action to be performed at site 312 through site control unit 320. The site control unit 320 confirms completion of the controller level command and the action request by obtaining control device status for the activated control device from one of controllers 321 (block 910). The control device status and action request status is sent from the SCU 320 to user system 314. The updated control device status is reflected in the Web Pages of GUI 513 (block 915). Processing for the user system / site control unit in this illustrative example ends at block 920.

Referring now to Figure 10, a first portion of the interaction between the processing logic in the central station 316 and the site system controller software 520 is illustrated. In this example, assume an event occurs in one of the control devices 322. Such an event could include a tripped sensor, an alarm activation, a status change notification, etc. As in a conventional alarm system, the event causes the alarm panel 430 to fault in an alarm condition (block 1010). The alarm panel 430 fault condition is detected by a sensor driver through device model 518. The sensor driver passes the fault condition to the real time event manager 516 in the SCU 320 (block 1015). The real time event manager 516 detects that the received fault condition is a security type of fault. A previously configured set of actions (i.e. an action request path) is initiated by the SCU 320 in response to this security fault (block 1020). Alternatively, a different action request path may be pre-configured in real time event manager 516 for handling other types of faults, such as fire events, status transitions, etc. In most cases, the action request path will include a step of updating database 317 with information related to the fault condition. In this case, a database update request is sent by the SCU 320 to one or more IP addresses corresponding to one or more databases 317 and one or more central stations 316 (block 1025). Upon receiving the database update request, the central station 316 updates the database 317. The information in

database 317 corresponding to the faulted control device is updated to reflect its new status (block 1030). Processing for the interaction between the SCU 320 and the central station 316 continues at the block labeled C shown in Figure 11.

Referring now to Figure 11, the processing for the interaction between the SCU 320 and the central station 316 continues at the bubble C. At this point, the database 317 has been updated by central station 316 to reflect the new status of the faulted control device. Alternatively or additionally, the central station 316 may alert its Web client software 614 to update database 317 across the network 310 (block 1110). The central station 316 also performs the remaining tasks in the action request path corresponding to the subject fault (block 1115). For example, an action request path for a particular type of fault may include various methods of notification including, sending an email to some predefined location to notify an individual of the fault, issuing a page or a telephone call, or other types of conventional actions in response to a fault. Finally, the central station 316 sends a status message back to the SCU 320 that originated the event. The status message serves as acknowledgement to the SCU 320 that the central station 316 satisfactorily handled the event (block 1120). Processing for the interaction between the SCU 320 and the central station 316 in this illustrative example terminates at block 1125.

Thus, a networked security system for network-based monitoring and control of an environment is disclosed. Although the present invention is described herein with reference to a specific preferred embodiment, many modifications and variations therein will readily occur to those with ordinary skill in the art. Accordingly, all such variations and modifications are included within the intended scope of the present invention as defined by the following claims.

CLAIMS

We claim:

1. A networked security apparatus comprising:

a site control unit for monitoring and controlling devices in an environment, the site control unit further including a site system controller for assembling device information into data packets for transfer on a network; and

a user system connected with the site control unit via the network for receiving the data packets from the site control unit via the network and for processing the data packets for access by a networked user.

2. The networked security apparatus as claimed in Claim 1 wherein the network is the Internet.

3. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a video capture unit for receiving video images and for digitizing the video images into a portion of the data packets.

4. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes an audio unit for receiving audio input and for digitizing the audio input into a portion of the data packets.

5. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a sensor input unit for receiving information from a plurality of sensors.

6. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a device controller for sending control information to a plurality of control devices.

7. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a graphical user interface generator for processing device information into displayable information.

8. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a sensor input unit for receiving information from a plurality of sensors, the site control unit further including a graphical user interface generator for generating displayable information including an abstraction symbol representing one or more of the plurality of sensors.

9. The networked security apparatus as claimed in Claim 8 wherein an activation of the abstraction symbol causes an activation of the corresponding sensor of the plurality of sensors.

10. The networked security apparatus as claimed in Claim 8 wherein one sensor of the plurality of sensors is a video camera.

11. The networked security apparatus as claimed in Claim 1 wherein the site control unit further includes a controller output unit for sending control information to a plurality of control devices, the site control unit further including a graphical user interface generator for generating displayable information including an abstraction symbol representing one or more of the plurality of control devices.

12. The networked security apparatus as claimed in Claim 11 wherein an activation of the abstraction symbol causes an activation of the corresponding control device of the plurality of control devices.

13. The networked security apparatus as claimed in Claim 11 wherein one control device of the plurality of control devices is a remotely controlled electrical power switch.

14. The networked security apparatus as claimed in Claim 3 wherein the site control unit further including a graphical user interface generator for generating displayable information derived from the information in the data packets, the graphical user interface generator further including a video module for displaying video images.

15. The networked security apparatus as claimed in Claim 1 wherein the user system further includes a security module for validating the authority of a user prior to granting access to the site control unit.

16. The networked security apparatus as claimed in Claim 1 further including:

a central station for communicating with the site control unit and the user system via the network, central station further including a database interface to a database, the database for storing information corresponding to the site control unit and the user system.

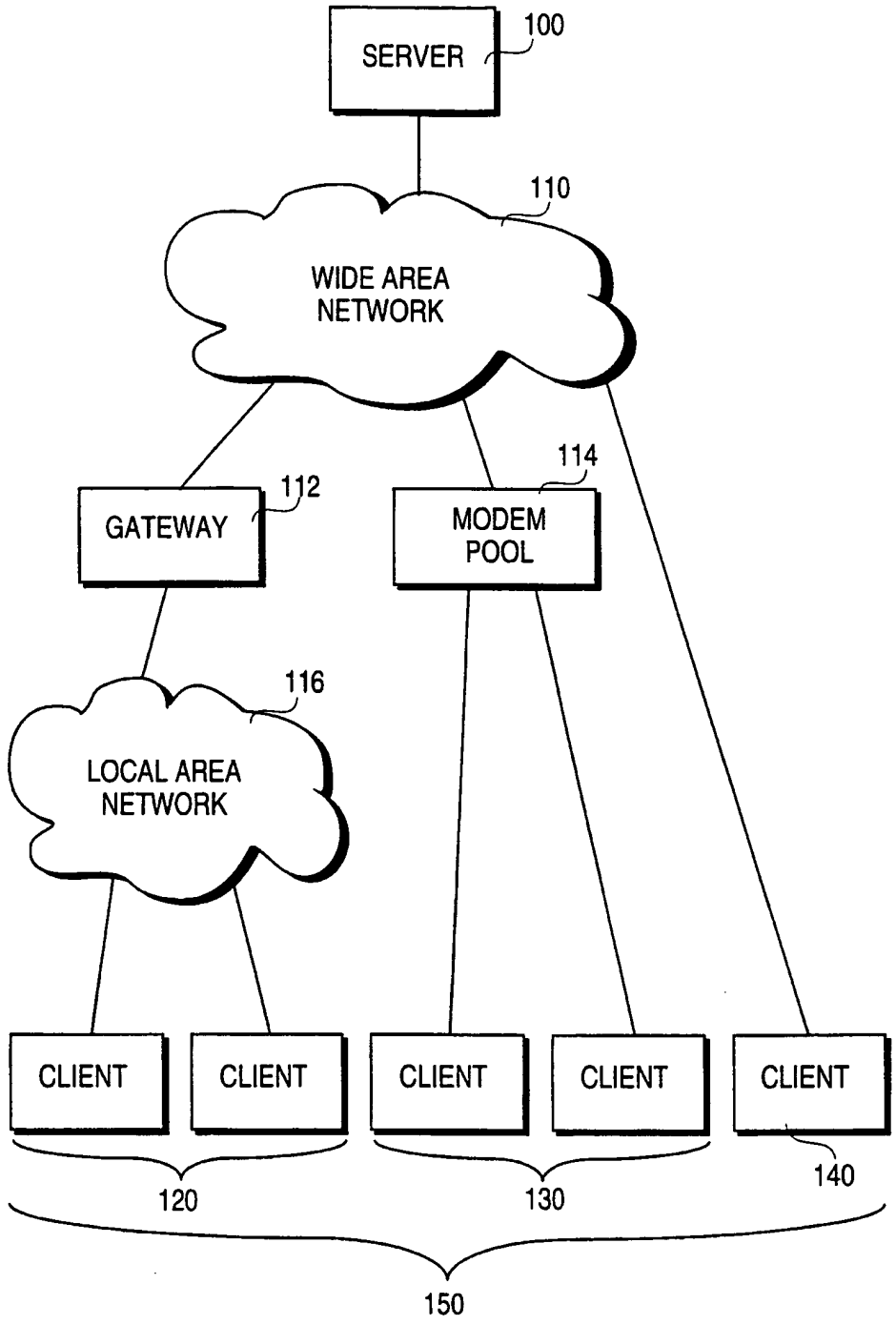



**FIG. 1** (PRIOR ART)

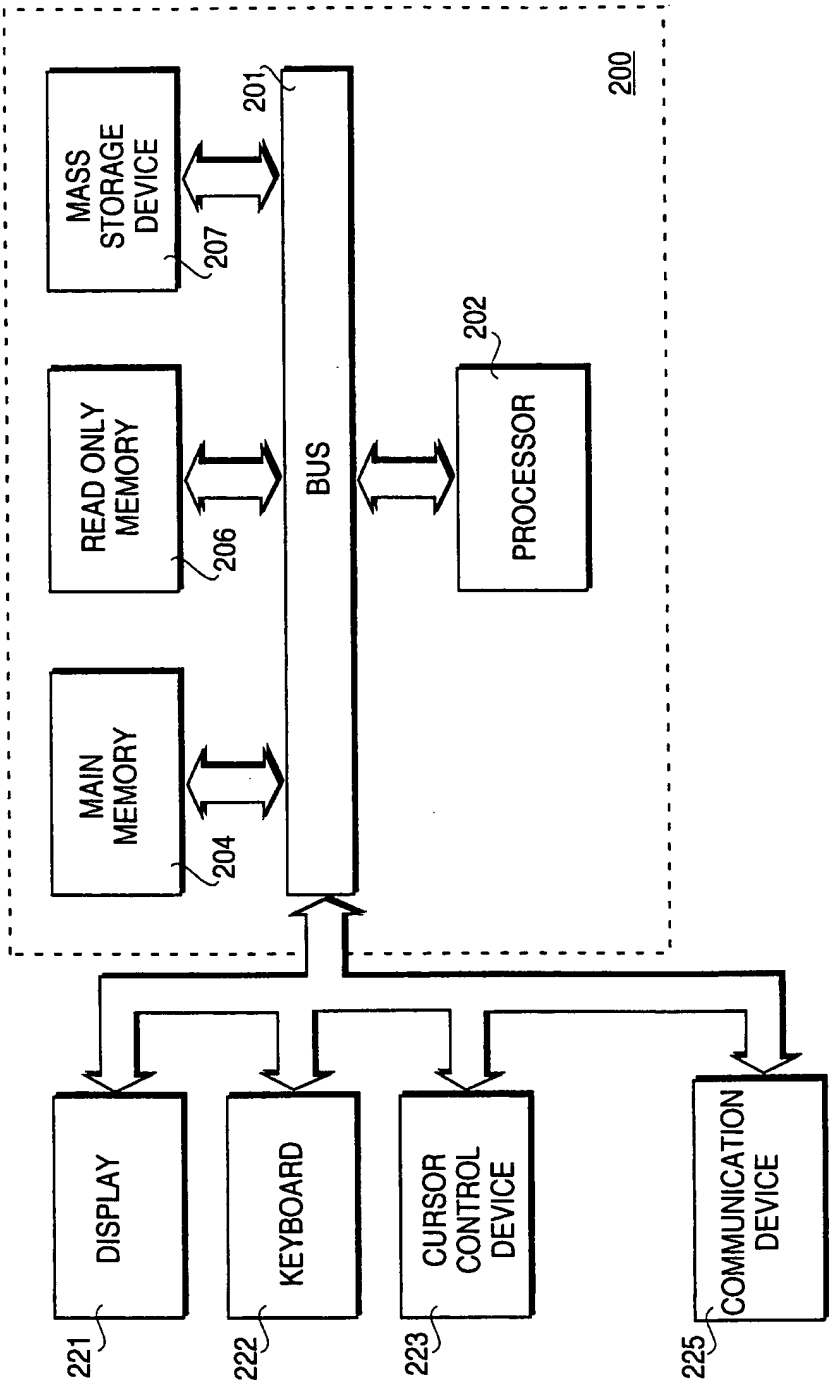



FIG. 2 (PRIOR ART)

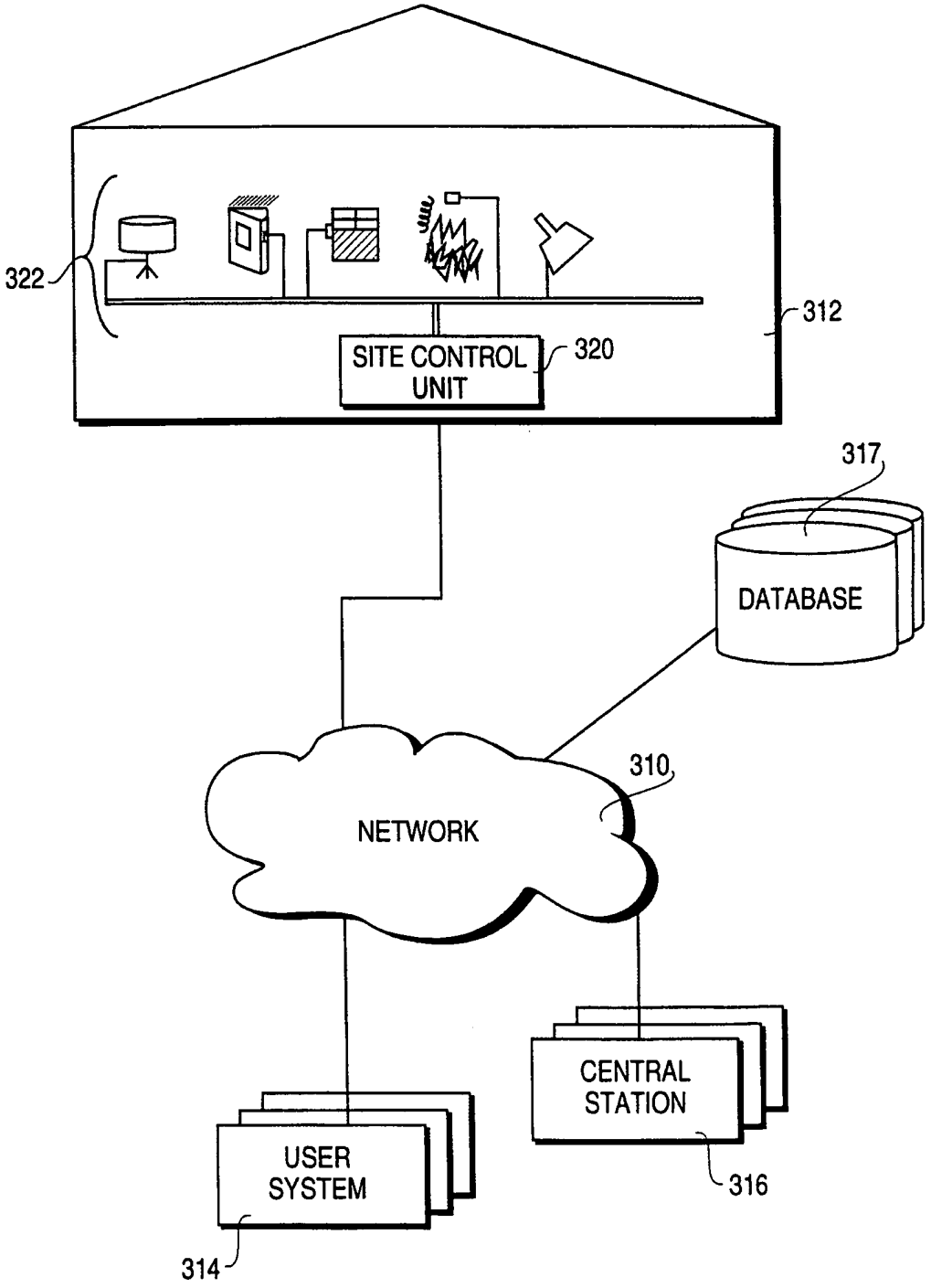

322
312
SITE CONTROL UNIT
320
317
DATABASE
310
NETWORK
CENTRAL STATION
316
USER SYSTEM
314

FIG. 3

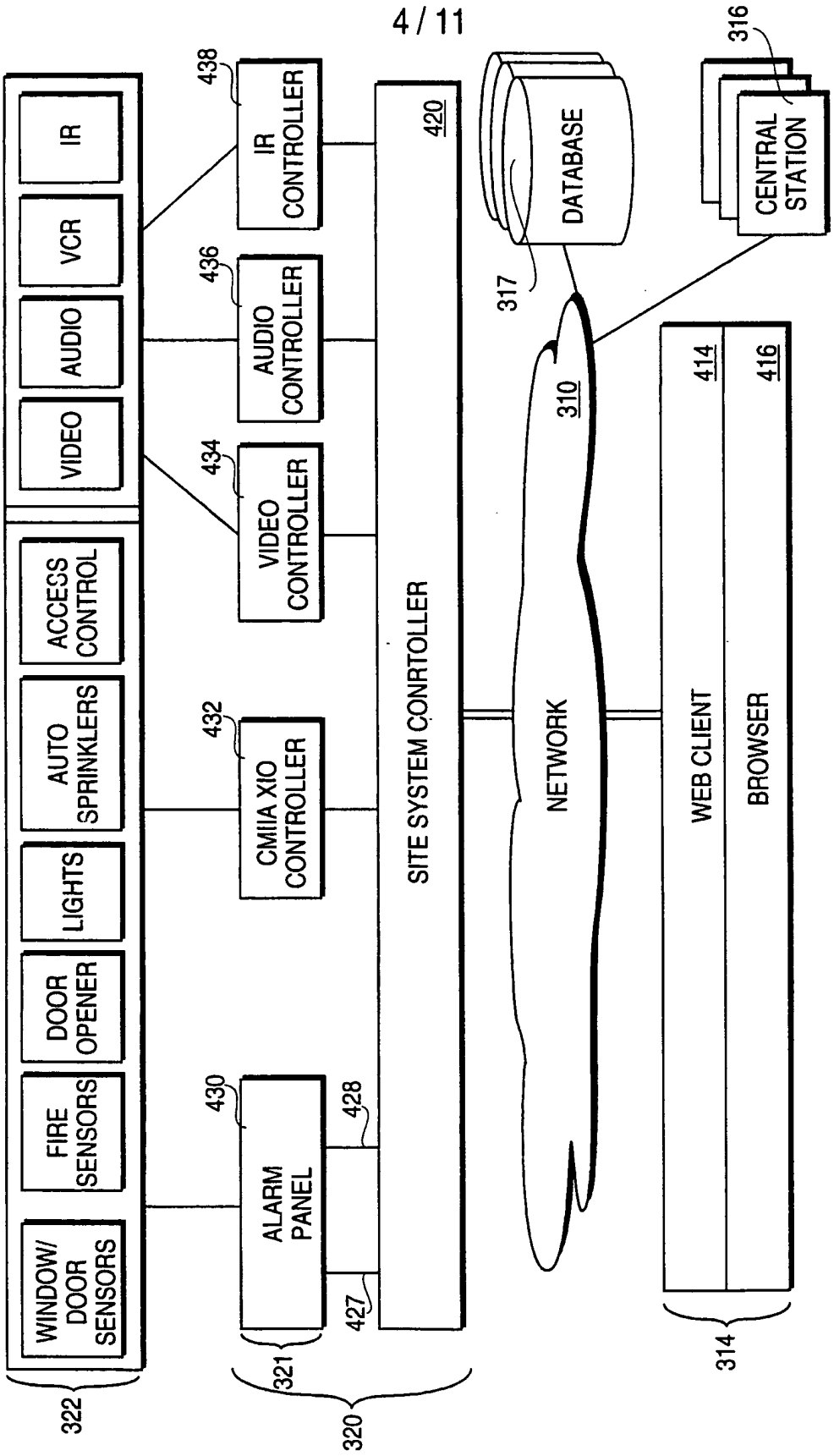

WINDOW/ DOOR SENSORS
FIRE SENSORS
DOOR OPENER
LIGHTS
AUTO SPRINKLERS
ACCESS CONTROL
VIDEO
AUDIO
VCR
IR
322
ALARM PANEL
430
428
427
321
CMIIA XIO CONTROLLER
432
VIDEO CONTROLLER
434
AUDIO CONTROLLER
436
IR CONTROLLER
438
320
SITE SYSTEM CONRTOLLER
420
NETWORK
310
DATABASE
317
CENTRAL STATION
316
WEB CLIENT
414
BROWSER
416
314

FIG. 4

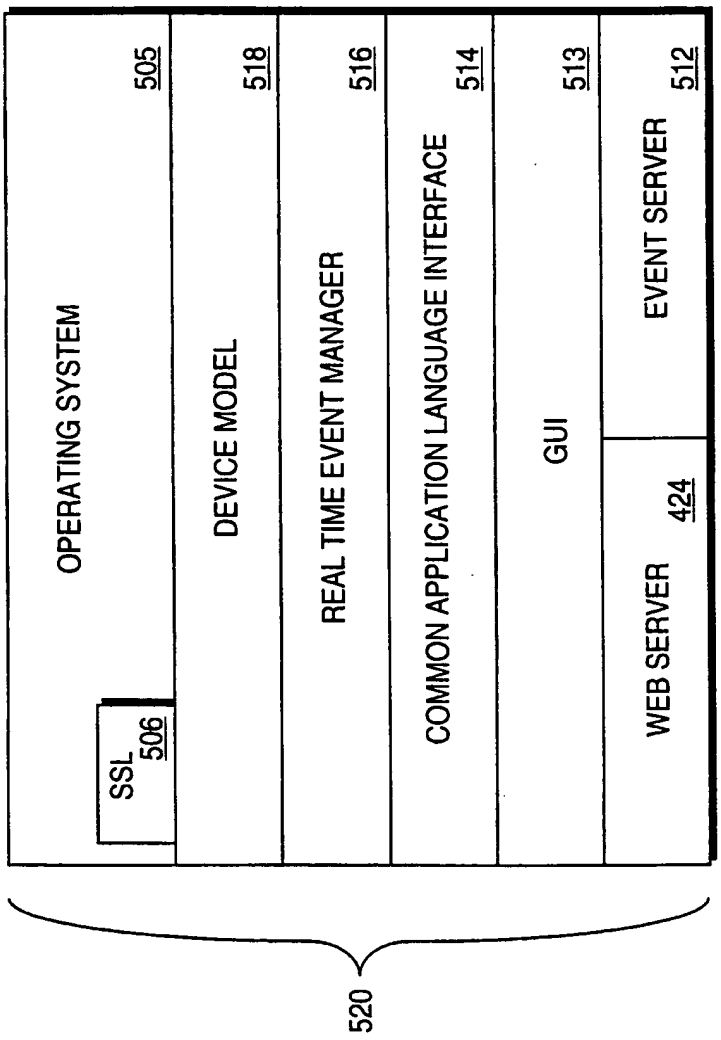

OPERATING SYSTEM
505
SSL
506
DEVICE MODEL
518
REAL TIME EVENT MANAGER
516
COMMON APPLICATION LANGUAGE INTERFACE
514
GUI
513
WEB SERVER
424
EVENT SERVER
512
520
SITE SYSTEM CONTROLLER
SOFTWARE ARCHITECTURE

FIG. 5

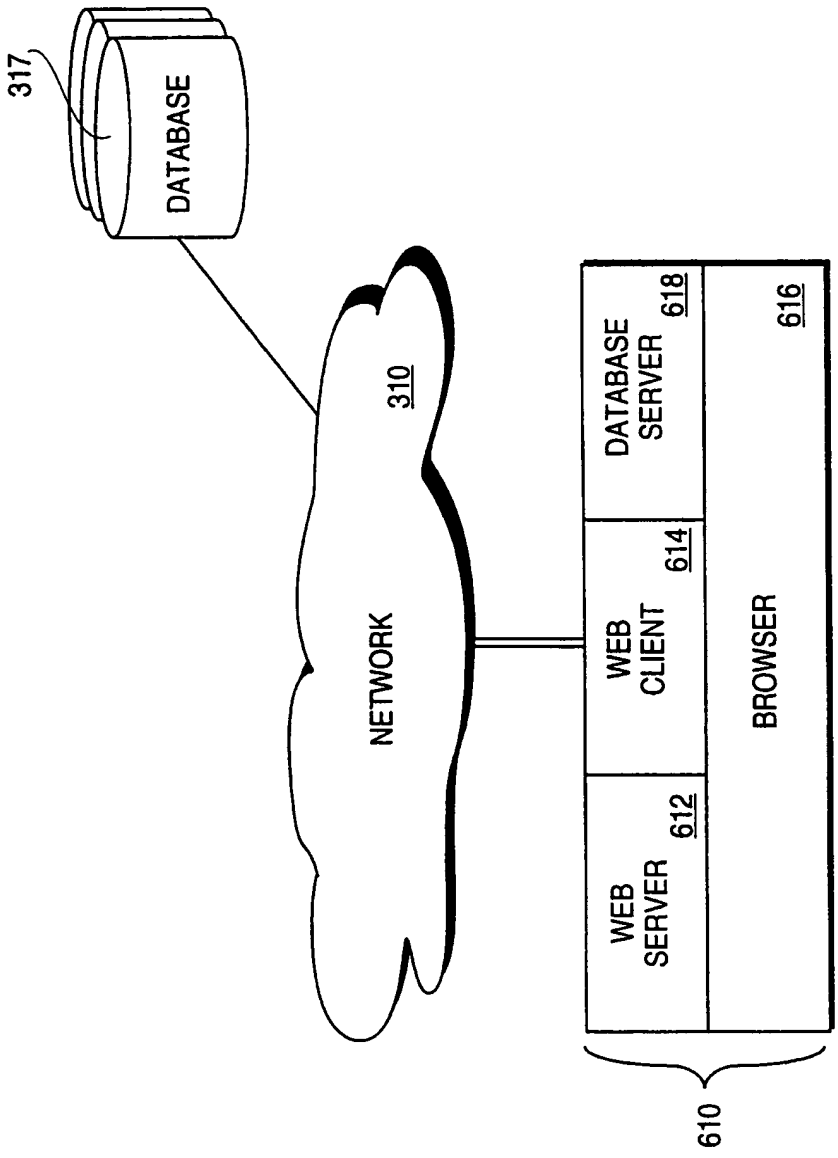



FIG. 6 CENTRAL STATION SOFTWARE ARCHITECTURE

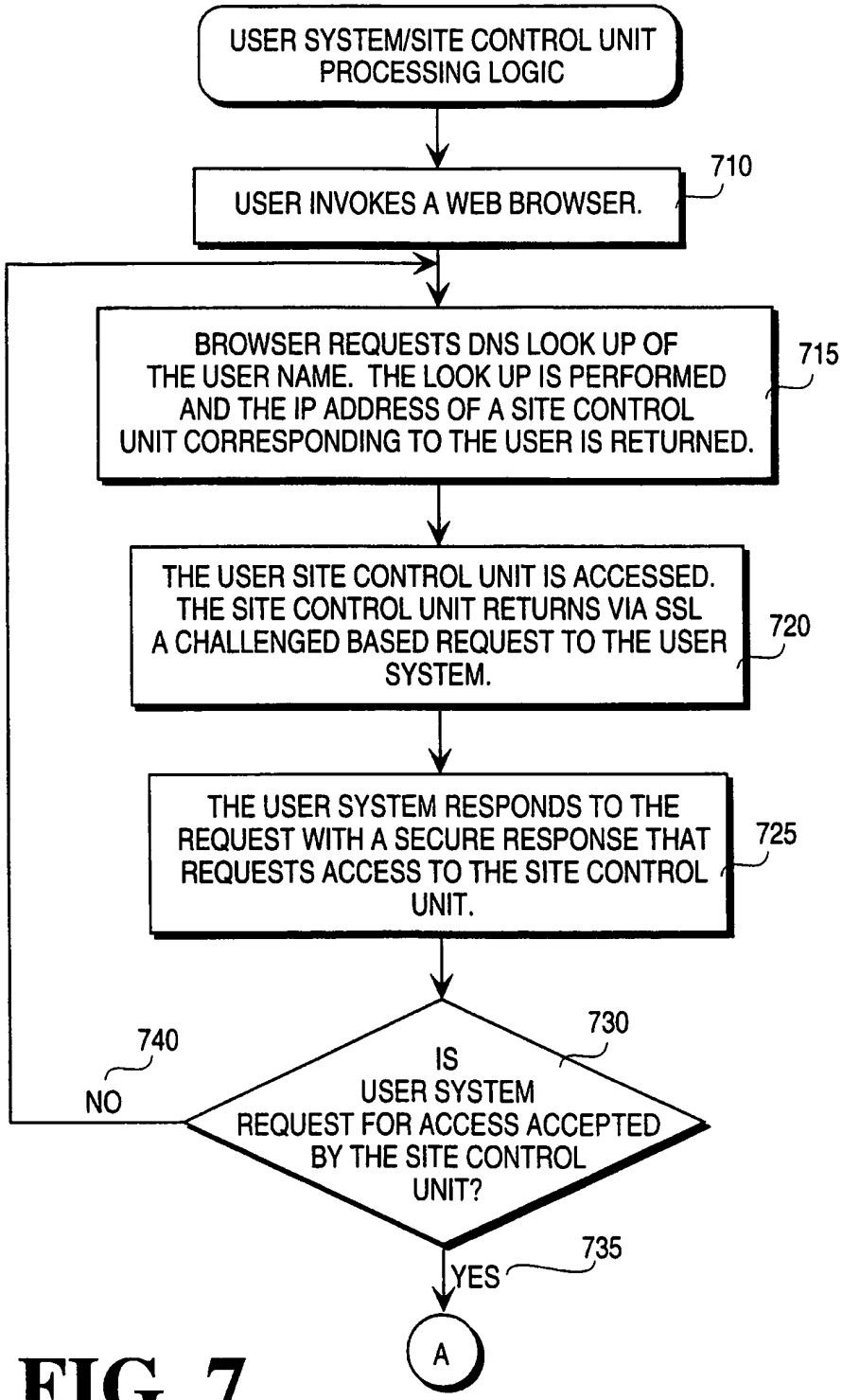

USER SYSTEM/SITE CONTROL UNIT PROCESSING LOGIC
USER INVOKES A WEB BROWSER.
710
BROWSER REQUESTS DNS LOOK UP OF THE USER NAME. THE LOOK UP IS PERFORMED AND THE IP ADDRESS OF A SITE CONTROL UNIT CORRESPONDING TO THE USER IS RETURNED.
715
THE USER SITE CONTROL UNIT IS ACCESSED. THE SITE CONTROL UNIT RETURNS VIA SSL A CHALLENGED BASED REQUEST TO THE USER SYSTEM.
720
THE USER SYSTEM RESPONDS TO THE REQUEST WITH A SECURE RESPONSE THAT REQUESTS ACCESS TO THE SITE CONTROL UNIT.
725
IS USER SYSTEM REQUEST FOR ACCESS ACCEPTED BY THE SITE CONTROL UNIT?
730
740
NO
YES
735
A

FIG. 7

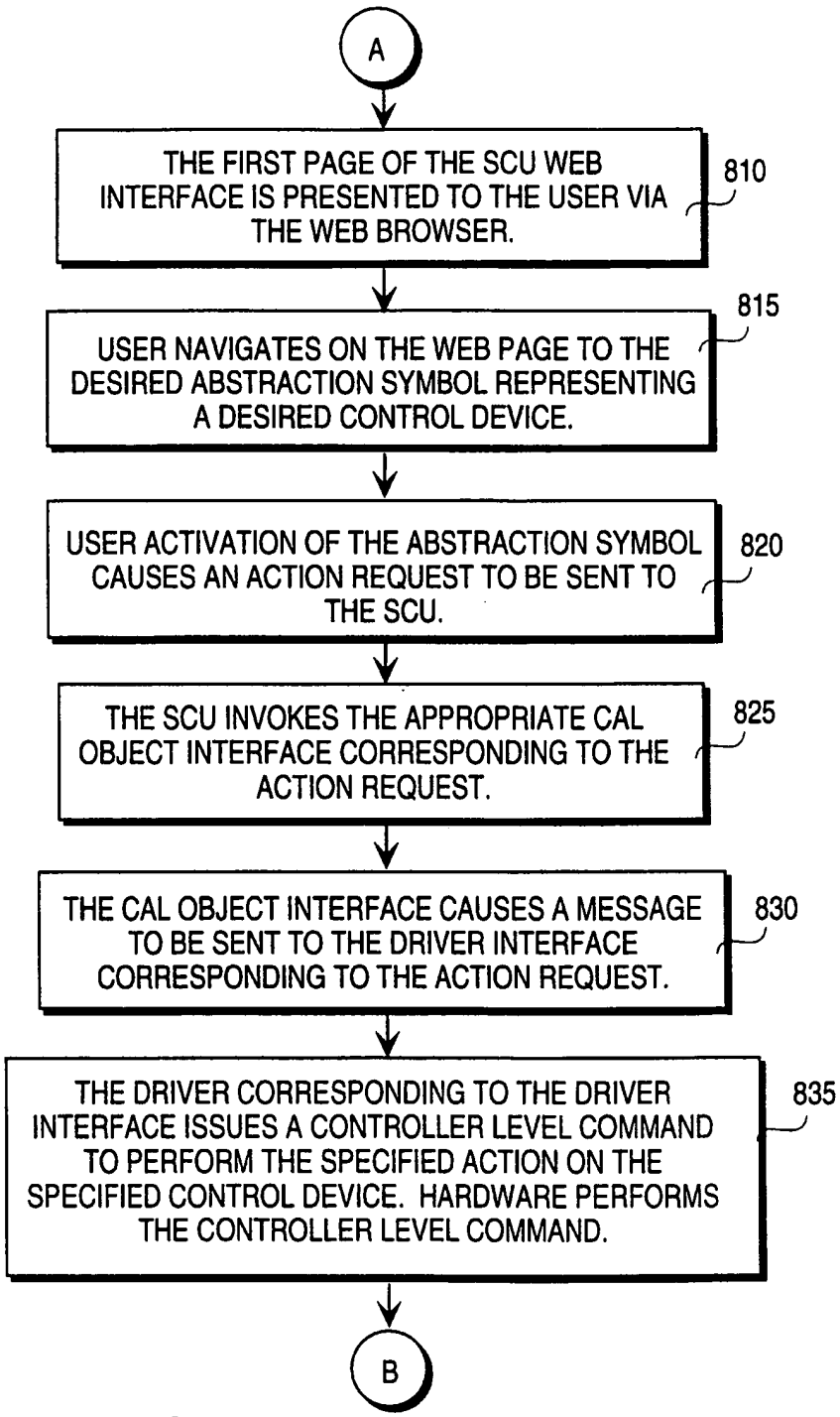

A
THE FIRST PAGE OF THE SCU WEB INTERFACE IS PRESENTED TO THE USER VIA THE WEB BROWSER.
810
USER NAVIGATES ON THE WEB PAGE TO THE DESIRED ABSTRACTION SYMBOL REPRESENTING A DESIRED CONTROL DEVICE.
815
USER ACTIVATION OF THE ABSTRACTION SYMBOL CAUSES AN ACTION REQUEST TO BE SENT TO THE SCU.
820
THE SCU INVOKES THE APPROPRIATE CAL OBJECT INTERFACE CORRESPONDING TO THE ACTION REQUEST.
825
THE CAL OBJECT INTERFACE CAUSES A MESSAGE TO BE SENT TO THE DRIVER INTERFACE CORRESPONDING TO THE ACTION REQUEST.
830
THE DRIVER CORRESPONDING TO THE DRIVER INTERFACE ISSUES A CONTROLLER LEVEL COMMAND TO PERFORM THE SPECIFIED ACTION ON THE SPECIFIED CONTROL DEVICE. HARDWARE PERFORMS THE CONTROLLER LEVEL COMMAND.
835
B

FIG. 8

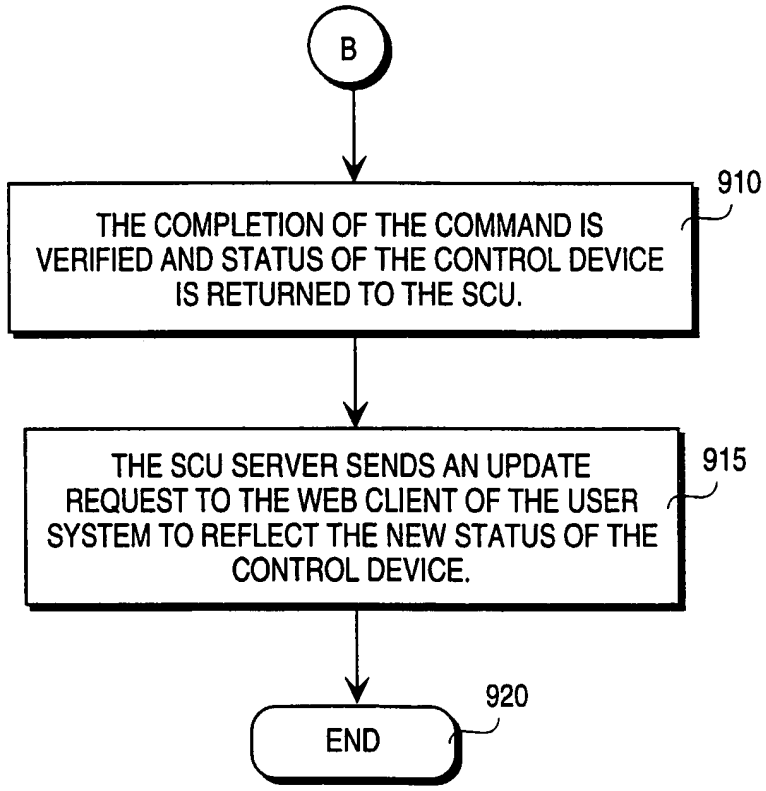
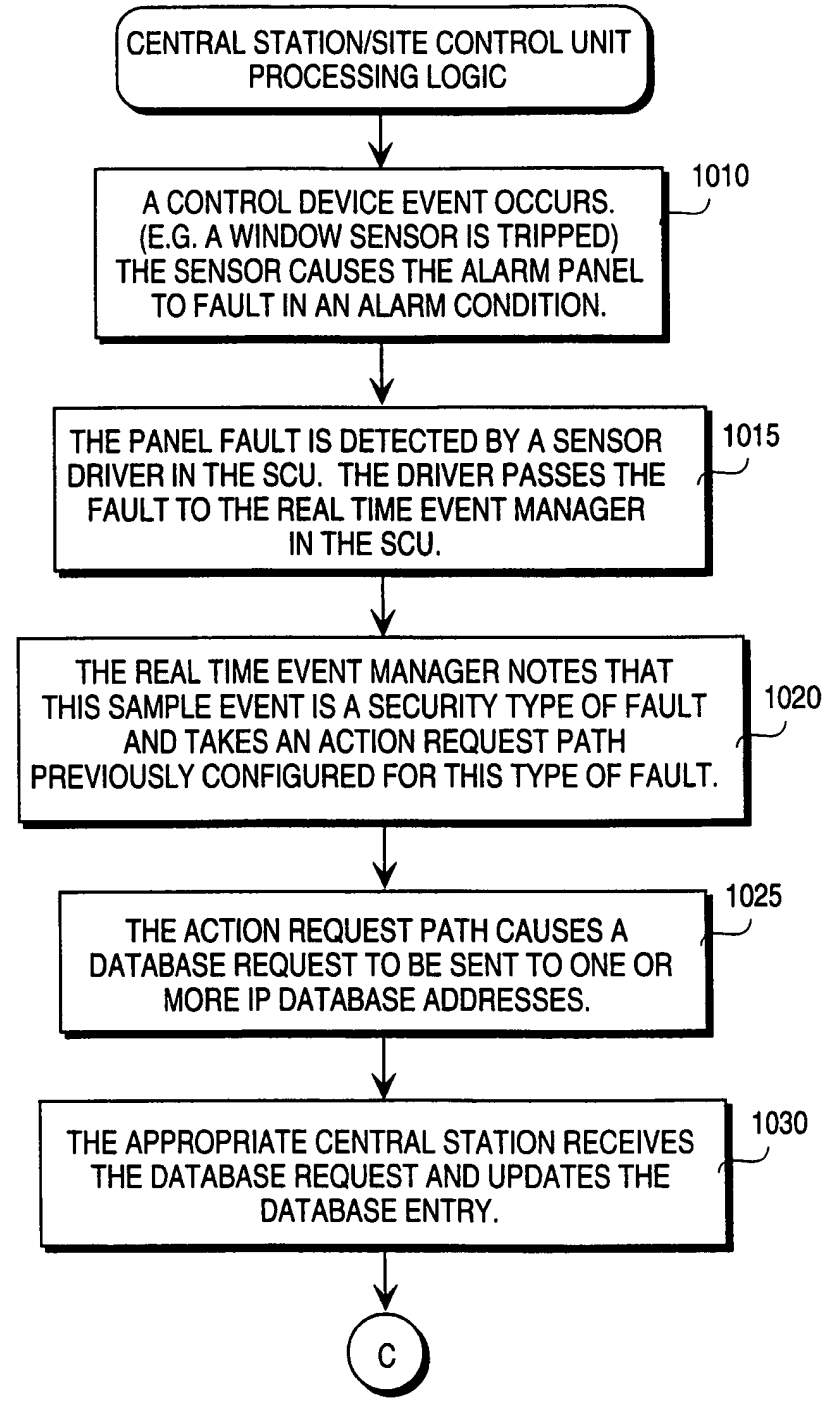
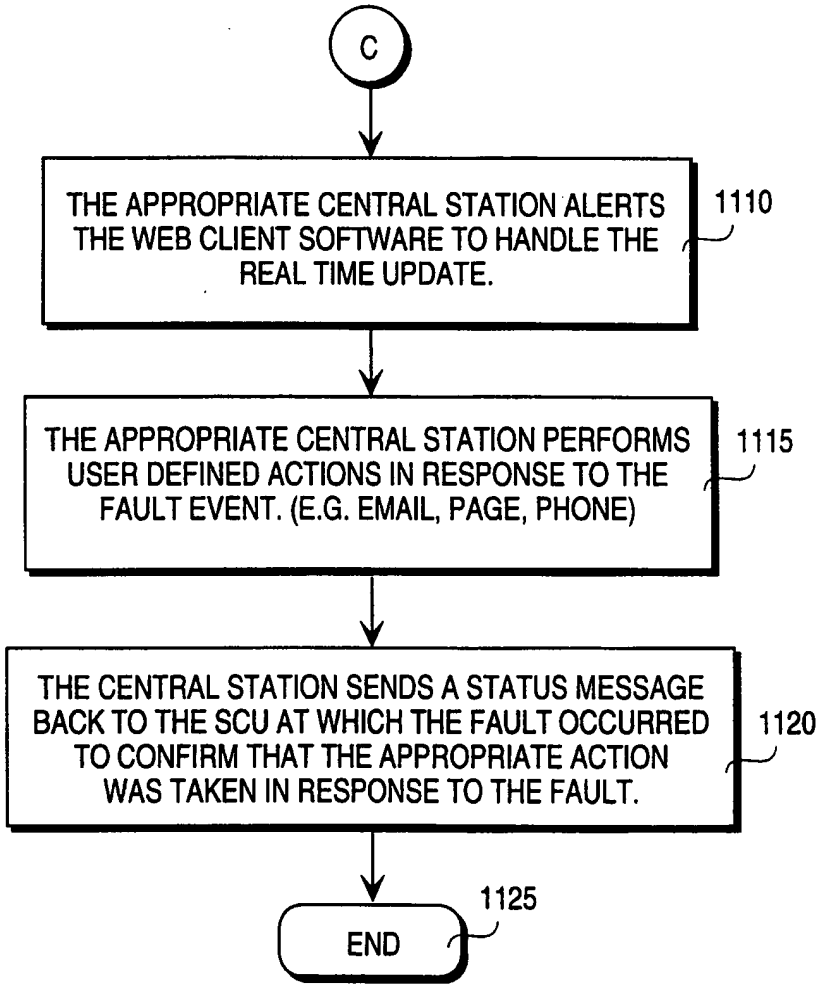

B
THE COMPLETION OF THE COMMAND IS VERIFIED AND STATUS OF THE CONTROL DEVICE IS RETURNED TO THE SCU.
910
THE SCU SERVER SENDS AN UPDATE REQUEST TO THE WEB CLIENT OF THE USER SYSTEM TO REFLECT THE NEW STATUS OF THE CONTROL DEVICE.
915
END
920

FIG. 9


CENTRAL STATION/SITE CONTROL UNIT PROCESSING LOGIC
A CONTROL DEVICE EVENT OCCURS. (E.G. A WINDOW SENSOR IS TRIPPED) THE SENSOR CAUSES THE ALARM PANEL TO FAULT IN AN ALARM CONDITION.
1010
THE PANEL FAULT IS DETECTED BY A SENSOR DRIVER IN THE SCU. THE DRIVER PASSES THE FAULT TO THE REAL TIME EVENT MANAGER IN THE SCU.
1015
THE REAL TIME EVENT MANAGER NOTES THAT THIS SAMPLE EVENT IS A SECURITY TYPE OF FAULT AND TAKES AN ACTION REQUEST PATH PREVIOUSLY CONFIGURED FOR THIS TYPE OF FAULT.
1020
THE ACTION REQUEST PATH CAUSES A DATABASE REQUEST TO BE SENT TO ONE OR MORE IP DATABASE ADDRESSES.
1025
THE APPROPRIATE CENTRAL STATION RECEIVES THE DATABASE REQUEST AND UPDATES THE DATABASE ENTRY.
1030
C

# FIG. 10


C
THE APPROPRIATE CENTRAL STATION ALERTS THE WEB CLIENT SOFTWARE TO HANDLE THE REAL TIME UPDATE.
1110
THE APPROPRIATE CENTRAL STATION PERFORMS USER DEFINED ACTIONS IN RESPONSE TO THE FAULT EVENT. (E.G. EMAIL, PAGE, PHONE)
1115
THE CENTRAL STATION SENDS A STATUS MESSAGE BACK TO THE SCU AT WHICH THE FAULT OCCURRED TO CONFIRM THAT THE APPROPRIATE ACTION WAS TAKEN IN RESPONSE TO THE FAULT.
1120
END
1125

# FIG. 11

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/01803

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :HO4N 7/18, 9/47; 7/10, 7/14

US CL :345/327; 348/211, 153, 159, 152, 154, 143

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. :

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS - camera, internet, sensors, control, packets, video, audio, security, suveillance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>--<br>Y | US 4,962,473 A (CRAIN) 09 October 1990, col. 4, lines 21-69, col. 5 lines 1-68, col. 6, lines 1-55, col. 8, lines 56-68, col. 9, lines 1-50 | 1-7, 14-16<br>----------<br>8-13 |
| A | US 5,206,732 A (HUDSON) 27 April 1993 | 1-16 |
| Y | US 4,992,866 A (MORGAN) 12 February 1991, col. 5, lines 11-48, fig. 2 | 8-13 |
| A | US 5,583,796 A (REESE) 10 December 1996 | 1-16 |
| A | US 5,491,511 A (ODLE) 13 February 1996 | 1-16 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | | | |
|---|---|---|---|
| * | Special categories of cited documents: | "T" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "A" | document defining the general state of the art which is not considered to be of particular relevance | "X" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "E" | earlier document published on or after the international filing date | "Y" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "L" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" | document member of the same patent family |
| "O" | document referring to an oral disclosure, use, exhibition or other means | | |
| "P" | document published prior to the international filing date but later than the priority date claimed | | |

| | |
|---|---|
| Date of the actual completion of the international search<br>21 MAY 1999 | Date of mailing of the international search report<br>15 JUN1999 |
| Name and mailing address of the ISA/US<br>Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231<br>Facsimile No. (703) 305-3230 | Authorized officer<br>Vivek Srivastava<br>Telephone No. (703) 305 - 4038 |

Form PCT/ISA/210 (second sheet)(July 1992)*